REMARKS

This Application has been carefully reviewed in light of the Office Action mailed October 31, 2005. In order to advance prosecution of this case, Applicants amend Claims 1, 4, 5, 10-15, and 17. Applicants also cancel Claims 2 and 3 without prejudice or disclaimer. Applicants previously canceled Claims 6, 7, 18, and 19 without prejudice or disclaimer. Applicants respectfully request reconsideration and favorable action in this case.

Section 102 Rejections

The Examiner rejects Claims 1-5 and 10-17 under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,398,196 issued to Chambers ("*Chambers*"). As amended, Claim 1 recites:

> A method of detecting viral code in subject files, comprising:
> creating an artificial memory region spanning one or more components of the operation system;
> creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values;
> emulating execution of at least a portion of computer executable code in a subject file;
> monitoring operating system calls by the emulated computer executable code;
> identifying an operating system call that the emulated computer executable code attempted to access; and
> deciding, based on the identified operating system call, whether the emulated computer executable code comprises viral code.

Chambers fails to recite, expressly or inherently, every element of amended Claim 1 for at least several reasons. First, *Chambers* fails to disclose "identifying an operating system call that the emulated computer executable code attempted to access." Second, *Chambers* also fails to disclose "deciding, based on the identified operating system call, whether the emulated computer executable code comprises viral code." For at least these reasons, as discussed in greater detail below, *Chambers* fails to recite every element of Claim 1.

First, *Chambers* fails to disclose "identifying an operating system call that the emulated computer executable code attempted to access." To the extent that the operation of the system disclosed by *Chambers* involves any use of operating system entry points, the *Chambers* system discloses only that:

> [T]he monitor program examines a list of operating system entry points to determine if any have changed as a result of the instruction just emulated. This would indicate that the target program had replaced an interrupt handler with a routine of its own. f there is such a chance, then it is logged at block 820. At block 820 a flag is also preferable set to indicate that the entry point has changed, so that the change will not be logged redundantly later. In some embodiments, the flag indicates that the new value of the entry point, so the monitor program can determine if the entry point gets modified yet again.
>
> Col. 9, ll. 21-32.

Thus, the monitor program of *Chambers* merely determines whether any operating system entry points have been modified. The monitor program does not "identif[y] an operating system call that the emulated computer executable code attempted to access" as the monitor program indiscriminately determines whether *any* of the operating system entry points in the list have changed. As a result, *Chambers* fails to recite "identifying an operating system call that the emulated computer executable code attempted to access" as recited by amended Claim 1.

Second, *Chambers* fails to disclose "deciding, based on the identified operating system call, whether the emulated computer executable code comprises viral code." Because *Chambers* fails to "identify" any operating system call, *Chambers* fails to disclose "deciding, based on the identified operating system call, whether the emulated computer executable code comprises viral code." As noted above, *Chambers* indiscriminately determines whether *any* operating system entry points in a list of operating system entry points have been modified. To whatever extent the monitor program of *Chambers* determines whether a target program is viral, the monitor program does not do this "based on [an] identified operating system call." As a result, *Chambers* also fails to "decid[e], based on the identified operating system call, whether the emulated computer executable code comprises viral code" as recited by amended Claim 1.

As a result, *Chambers* fails to recite, either expressly or inherently, every element of amended Claim 1. Claim 1 is thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claim 1 and its dependents.

Although of differing scope from Claim 1, Claims 10-12 and 14 include elements that, for reasons substantially similar to those discussed with respect to Claim 1, are not recited by *Chambers*. Claims 10-12 and 14 are allowable for at least these reasons.

Applicants respectfully request reconsideration and allowance of Claims 10-12 and 14, and their respective dependents.

Additionally, Applicants cancel Claims 2 and 3 without prejudice or disclaimer, thereby obviating the Examiner's rejection of Claims 2 and 3. Applicants respectfully note, however, that, with respect to all cancellations and amendments herein, Applicants reserve the right to pursue broader subject matter than is currently claimed through the filing of continuations and/or other related applications.

Section 103 Rejections

The Examiner rejects Claims 8, 9, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Chambers in view of U.S. Patent No. 5,974,549 issued to Golan ("*Golan*"). Claims 8 and 9 depend from Claim 1, while Claim 20 depends from Claim 14. Claims 1 and 14 are shown above to be allowable. Claims 8, 9, and 20 are thus allowable for at least these reasons. Applicants respectfully request reconsideration and allowance of Claims 8, 9, and 20.

Conclusions

Applicants have made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other reasons clearly apparent, Applicants respectfully request full allowance of all pending Claims. If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, the undersigned attorney for Applicants stands ready to conduct such a conference at the convenience of the Examiner.

No fees are believed to be due, however, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.
Attorneys for Applicants

Todd A. Cason
Reg. No. 54,020

2001 Ross Avenue, Suite 600
Dallas, Texas 75201-2980
(214) 953-6452

Date: 1-30-06

CORRESPONDENCE ADDRESS:

Customer Number: **05073**